BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 30 098.4
Anmeldetag:	04. Juli 2002
Anmelder/Inhaber:	Siemens Aktiengesellschaft, München/DE
Bezeichnung:	Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt, insbesondere einem Fahrzeug gegenüber wenigstens einem Schlüssel
IPC:	H 04 B, G 08 C

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 28. November 2002
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Weihmayr

A 9161
06/00
EDV-L

Beschreibung

Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt, insbesondere einem Fahrzeug gegenüber wenigstens einem Schlüssel

Die Erfindung betrifft ein Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt. Derartige Verfahren finden beispielsweise in der Fahrzeugtechnik Anwendung, wobei ein Fahrzeug gegenüber einem Schlüssel bzw. ID-Geber authentifiziert werden soll.

Diese Authentifizierung, also der Nachweis der Berechtigung, erfolgt üblicherweise mittels einer bidirektionalen, verschlüsselten Kommunikation zwischen dem Fahrzeug bzw. der darin befindlichen Basisstation, beispielsweise ein Steuergerät, und dem von einer Person mitgeführten Schlüssel.

Hierbei werden die Anforderungen gegen unbefugten Zugang immer höher, so dass auch mit einem Abhören und Entschlüsseln der Authentifizierung gerechnet werden muss.

Zur Erhöhung der Sicherheit gegen einen unbefugten Zugang ist in der DE 19516992C1 beispielsweise ein bidirektionales Verfahren vorgeschlagen, bei dem ein Schlüssel bzw. ein Transponder zunächst ungültige Daten zu einem Schloss bzw. einem Steuergerät sendet, woraufhin ein Aufforderungssignal mit einer Speicheradresse zu dem Transponder zurückgesendet wird. Das im Transponder unter der Speicheradresse abgespeicherte Codewort wird ausgelesen und zum Schloss gesendet. Dort wird das Codewort mit einem Sollcodewort verglichen und bei Übereinstimmung eine Wegfahrsperre freigegeben. Anschließend werden Adresse und/oder Codewort im Schloss neu berechnet und im Transponder für den nachfolgenden Freigabezyklus eingestellt, so dass ein Wechselcode entsteht.

Derartige Verfahren zur Zugangsberechtigung (inkl. Authentifizierung) bieten bei der schnell fortschreitenden Abhör- und Entschlüsselungstechnik allerdings nur einen bedingten Schutz bzw. müssen immer aufwändiger gestaltet werden, um einen ausreichenden Schutz zu gewährleisten.

Insbesondere bei passiven Zugangssystemen, beispielsweise in der Fahrzeugtechnik, bei denen durch einen tragbaren ID-Geber bzw. Schlüssel ohne (aktives) Betätigen eines Schlüsselknopfes das Fahrzeug verriegelt und entriegelt werden kann (mit eventuell gleichzeitiger Aktivierung und Deaktivierung der Wegfahrsperre bzw. Diebstahlsicherung), ergeben sich neue Probleme.

Beispielsweise kann ein Schlüssel, der im Fahrzeuginneren vergessen oder absichtlich deponiert wurde, dazu führen, dass bei einem Auslösen einer Kommunikation, beispielsweise durch ein Ziehen am Türgriff, zwischen Fahrzeug und vermeintlich berechtigter Person mit gültigem Schlüssel, eine unbefugte Person Zutritt erhält. Zieht nämlich eine unbefugte Person am Türgriff, so wird üblicherweise von einer im Fahrzeug befindlichen Basisstation abgefragt, ob sich ein gültiger Schlüssel in der Nähe befindet.

Selbst bei induktiver Übertragung mit entsprechenden induktiven Antennen, welche üblicherweise im Bereich der Türschlösser angeordnet sind, kann aber aus physikalischen Gründen nicht verhindert werden kann, dass das Empfangsfeld auch zum Teil in das Fahrzeuginnere reicht. Bei entsprechender Lage des im Fahrzeug befindlichen Schlüssels würde nach einem Auslösen die Kommunikation dann mit diesem Schlüssel erfolgen, so dass eine unbefugte Person Zutritt zum Fahrzeug erhalten könnte.

Um zu verhindern, dass statt eines mitgeführten Schlüssels ein im Fahrzeug befindlicher Schlüssel als gültiger Schlüssel

erkannt wird, ist es notwendig, derartige Schlüssel als zumindest zeitweise ungültig bzw. deaktiviert zu markieren.

Diese Markierung erfolgt üblicherweise mittels einer bidirektionalen Kommunikation und Speicherung der erhaltenen Information im Steuergerät, wobei zumindest die Kommunikation von Schlüssel in Richtung Steuergerät mittels einer RF-Strecke erfolgt. Sollen der oder die deaktivierten Schlüssel wieder aktiviert werden, wird diese Markierung wieder aufgehoben.

Eine derartige Authentifizierung ist jedoch aufwändig und dennoch, insbesondere aufgrund der weitreichenden RF-Strecke, gegen aufwändige Abhörversuche anfällig.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt, insbesondere einem Fahrzeug gegenüber wenigstens einem Schlüssel, zu schaffen, das einen erhöhten Schutz gegen eine unbefugte Authentifizierung bietet und auf einfache Art und Weise zu realisieren ist.

Diese Aufgabe wird erfindungsgemäß mit einem Verfahren mit den Merkmalen des Anspruchs 1 gelöst.

Nach dem erfindungsgemäßen Verfahren werden Schlüssel nicht im Steuergerät als aktiviert bzw. deaktiviert gekennzeichnet, sondern mittels einer unidirektionalen Kommunikation im Schlüssel selbst. Vorteilhafterweise findet diese Kommunikation nur über eine induktive LF-Strecke (mit einer Frequenz von beispielsweise 10 bis 200 kHz) mit geringer Reichweite, beispielsweise unter 2 m, statt. Durch die Übertragung in nur einer Richtung und zudem über eine LF-Strecke kann vorteilhafterweise eine erhöhte Sicherheit gegenüber Abhören erreicht werden.

Zudem ist nach dem erfindungsgemäßen Verfahren trotz der unidirektionalen Übermittlung die Authentifizierung kryptologisch abgesichert, indem im Schlüssel ein Ergebnis aus übermittelten Daten berechnet wird und mit einem übermittelten Ergebnis verglichen wird.

Die Sicherheit kann hierbei durch ein nicht oder nur schwer entschlüsselbares Berechnungsverfahren (Rechenalgorithmus), wie beispielsweise eine Berechnung nach dem Hash-Verfahren, mit einem Code- bzw. Schlüsselwort, erhöht werden.

Zudem ist erfindungsgemäß das übermittelte Rechenergebnis abhängig von einem inkrementierbaren oder dekrementierbaren Datum, wie beispielsweise Hoch- oder Herunterzählen eines Zählerstandes oder einer Zeitangabe, so dass ein vorhergehendes übermitteltes Berechnungsergebnis automatisch ungültig ist. Hierdurch wird die Sicherheit gegen eine unbefugte Authentifizierung weiter erhöht, da selbst ein Abhören einer Übermittlung und somit Kenntnis eines Rechenergebnisses keine Rückschlüsse auf ein von da an gültiges (neues) Rechenergebnis zulässt.

Das erfindungsgemäße Verfahren kann in einer Ausgestaltung der Erfindung zur Authentifizierung eines ersten zumindest zeitweise stationären Objektes, beispielsweise ein Fahrzeug, gegenüber wenigstens einem weiteren mobilen Objekt, beispielsweise ein Fahrzeugschlüssel, verwendet werden. So können Schlüssel, die deaktiviert wurden, da sie in einem abgesperrten Fahrzeug verblieben sind oder aus anderen Gründen zumindest zeitweise als ungültig angesehen werden sollen, nach dem erfindungsgemäßen Verfahren auf einfache Art und Weise mit hochgradiger Abhörsicherheit und zusätzlicher kryptologischer Absicherung wieder aktiviert werden, also das Fahrzeug gegenüber einem solchen Schlüssel authentifiziert werden.

Da die kryptologische Sicherheit durch Berechnung im Schlüssel erfolgt und das jeweils übermittelte Rechenergebnis für zukünftige Authentifizierungen ungültig ist, kann die unidirektionale Übermittlung vorteilhafterweise in einem einfacher zu realisierenden Klartext erfolgen.

Selbstverständlich ist das erfindungsgemäße Verfahren nicht auf das Aktivieren vorher deaktivierter Schlüssel, beispielsweise durch ein Entriegeln bzw. Aufsperren des Fahrzeuges durch einen gültigen aktiven Schlüssel, beschränkt.

Das erfindungsgemäße Verfahren lässt sich auch auf eine Authentifizierung eines Schlüssels gegenüber einem Fahrzeug anwenden. Ebenso ist es denkbar, die Authentifizierung nicht nur zur Aktivierung von im Fahrzeug verbliebenen und deaktivierten Schlüsseln zu verwenden, sondern beispielsweise einer jeden (nachfolgenden) meist bidirektionalen Kommunikation zwischen den Objekten, beispielsweise zum Auslösen gewünschter Funktionen, wie „Ent- bzw. Verriegeln der Zentralverriegelung", „Deaktivieren bzw. Aktivieren der Wegfahrsperre" usw., vorzuschalten.

Weitere vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Die Erfindung wird nachfolgend anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

In der Zeichnung zeigt:

Fig. 1 ein Ablaufdiagramm des erfindungsgemäßen Verfahrens.

Wie in Fig. 1 als Ablaufdiagramm dargestellt, beginnt das erfindungsgemäße Verfahren mit einem Start, also einem Auslösen, wie beispielsweise durch ein Ziehen einer Bedienperson

am Türgriff und Detektieren eines gültigen (aktiven) Schlüssels durch das Fahrzeug bzw. das im Fahrzeug befindliche Steuergerät. Bei einem solchen Öffnen kann dann ein Aktivierungssignal (enable) für deaktivierte (disabled) Schlüssel ausgesandt werden.

Es ist aber auch denkbar, einen solchen Start auf andere Art, beispielsweise durch den Bediener selbst bzw. durch Betätigen einer entsprechenden Taste oder Schalters am oder im Fahrzeug oder in Abhängigkeit einer anderen vom Steuergerät auszuführenden Aktion wie „Einschalten der Innenraumbeleuchtung" etc., herbeizuführen.

Einmal gestartet wird vom Steuergerät bzw. der Basisstation im Fahrzeug eine entsprechende Information in Form eines Sendetelegramms (ST) ausgesandt, welches aus einer Zufallszahl (ZZ), einem inkrementierbaren Datum wie beispielsweise ein Zählerstand (ZS), einem Rechenergebnis (RE) und einem Funktionscode (FC) besteht.

Die Zufallszahl wird im Steuergerät bei jeder Übertragung neu ermittelt und der Zählerstand eines im Steuergerät vorhandenen Zählers nach jedem Aussenden beispielsweise um 1 inkrementiert oder dekrementiert. Selbstverständlich ist es auch möglich, statt einem Zählerstand eine Zeitangabe einer im Steuergerät vorwärts oder rückwärts laufenden Uhr zu übermitteln, so dass nach jedem Aussenden anstatt eines neuen weiter fortgeschrittenen (vorwärts oder rückwärts) Zählerstandes eine neue Zeitangabe mitübermittelt wird.

In einem deaktivierten Schlüssel wird das Sendetelegramm, welches vorteilhafterweise über eine in ihrer Reichweite begrenzte, in den Innenraum gerichtete, induktive Antenne abgestrahlt wird, empfangen, wobei der Schlüssel intervallartig empfängt oder aufgrund des geringen Strombedarfs für einen LF-Empfänger sogar permanent empfangen kann.

Um unnötige Berechnungen im Schlüssel bzw. der darin enthaltenen Elektronik mit Logik vorteilhafterweise zu vermeiden, kann nachfolgend überprüft werden, ob der empfangene Zählerstand größer (im Falle eines vereinbarten Dekrementierens entsprechend kleiner) als der im Schlüssel gespeicherte Zählerstand ist. Der in einem Register im Schlüssel gespeicherte Zählerstand stammt hierbei beispielsweise von einer vorangegangenen Authentifizierung oder noch vom einmaligen Synchronisieren der Schlüssel mit dem Steuergerät in Form eines Anlernens bzw. einer Initialisierung.

Ist der empfangene Zählerstand größer (oder im Falle eines Abwärtszählers im Steuergerät kleiner) als der gespeicherte Zählerstand, so findet im Schlüssel die Berechnung eines Rechenergebnisses aus dem übermittelten Zählerstand, aus der übermittelten Zufallszall und eventuell aus weiteren in dem übermittelten Funktionscode enthaltenen Informationen statt.

Ist der empfangene Zählerstand dagegen kleiner oder gleich (bzw. bei einem Abwärtszähler statt einem Aufwärtszähler größer oder gleich) dem gespeicherten Zählerstand, so findet im Schlüssel keine Berechnung statt und der Schlüssel wartet weiterhin auf ein neues Sendetelegramm.

Für die Berechnung wird mittels eines im Schlüssel bekannten nicht umkehrbaren (Verschlüsselungs-)Rechenalgorithmus, wie beispielsweise ein Hash-Algorithmus, mit einem ebenfalls im Schlüssel bekannten Schlüsselwort ein Rechenergebnis berechnet und nachfolgend mit dem übermittelten Rechenergebnis verglichen.

Stimmen das übermittelte und das berechnete Rechenergebnis nicht überein, so finden im Schlüssel keine weiteren Aktionen statt (Stop), so dass der Schlüssel wieder auf den Empfang eines Sendetelegramms wartet.

Stimmen die Rechenergebnisse dagegen überein, so wird im Schlüssel der übertragene Zählerstand (oder die Zeitangabe) beispielsweise in einem Register, einem Flashspeicher o.ä., abgespeichert und der Schlüssel durch eine Aktion im Schlüssel, beispielsweise mittels Änderung eines Registerwertes oder des Inhalts einer Speicheradresse, Schalten eines Schaltkreises etc., aktiviert (enabled).

Mit einem derart aktivierten Schlüssel lassen sich Aktionen wie „Ent- bzw. Verriegeln der Zentralverriegelung", „Deaktivieren bzw. Aktivieren der Wegfahrsperre", „Fahrzeug entsichern bzw. sichern„ usw., mit für passive Zugangssysteme bekannten Übertragungsverfahren ausführen, nachdem die Berechtigung bzw. die Authentifizierung erfolgt ist.

Selbstverständlich ist das erfindungsgemäße Verfahren nicht auf das dargestellte Ausführungsbeispiel begrenzt, sondern lässt sich auf alle Gebiete übertragen, in denen ein Objekt gegenüber wenigstens einem weiterem Objekt auf einfache Art und Weise bei hoher Sicherheit gegenüber Fehlern und Angriffen von Unbefugten authentifiziert werden soll.

So kann das erfindungsgemäße Verfahren auch bei Haustüren, Garagentoren, Zutritt zu Sicherheitsbereichen u.ä. angewendet werden.

Patentansprüche

1. Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt, insbesondere einem Fahrzeug gegenüber einem Schlüssel,

   a) bei dem eine Information zwischen dem ersten Objekt und dem wenigstens einen weiteren Objekt unidirektional übertragen wird,

   b) aus Teilen der übertragenen Information in dem jeweiligen empfangenden Objekt ein Rechenergebnis berechnet wird,

   c) das berechnete Rechenergebnis mit einem mit der Information mitübertragenen Rechenergebnis verglichen wird,

   d) nur bei Übereinstimmung das jeweils sendende Objekt als authentifiziert angesehen wird und

   e) das Rechenergebnis für weitere Übermittlungen ungültig erklärt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass als erstes Objekt von einem Fahrzeug Information ausgesendet und als wenigstens ein weiteres Objekt von einem Schlüssel empfangen wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass als Teile der Information eine Zufallszahl und ein inkrementier- oder dekrementierbares Datum, welches in dem wenigstens einen weiteren Objekt bei Übereinstimmung der Rechenergebnisse gespeichert wird, übermittelt werden und dass nach jedem Aussenden der Information, unabhängig

von einem erfolgreichen Empfangen, das Datum vor einem erneuten Aussenden inkrementiert oder dekrementiert wird.

4. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass als inkrementierbares Datum ein Zählerstand oder Zeitdatum übermittelt wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Berechnung des Ergebnisses nur erfolgt, wenn das übermittelte Datum größer als das gespeicherte Datum ist.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass bei Übereinstimmung des übermittelten Ergebnisses und des berechneten Ergebnisses das inkrementierbare Datum erhöht wird, so dass das übermittelte Ergebnis ungültig wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Ergebnis in dem wenigstens einen weiteren Objekt anhand eines dort bekannten kryptologischen Rechenalgorithmus und eines Codeworts berechnet wird.

Zusammenfassung

Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt, insbesondere einem Fahrzeug gegenüber wenigstens einem Schlüssel

Die Erfindung betrifft ein Verfahren zur Authentifizierung eines ersten Objekts gegenüber wenigstens einem weiteren Objekt, insbesondere einem Fahrzeug gegenüber einem Schlüssel, bei dem eine Information zwischen dem ersten Objekt und dem wenigstens einen weiteren Objekt unidirektional übertragen wird, aus Teilen der übertragenen Information in dem jeweiligen empfangenden Objekt ein Rechenergebnis berechnet wird, das berechnete Rechenergebnis mit einem mit der Information mitübertragenen Rechenergebnis verglichen wird, nur bei Übereinstimmung das jeweils sendende Objekt als authentifiziert angesehen wird und das Rechenergebnis für weitere Übermittlungen ungültig erklärt wird.

Hauptzeichnung ist Figur 1

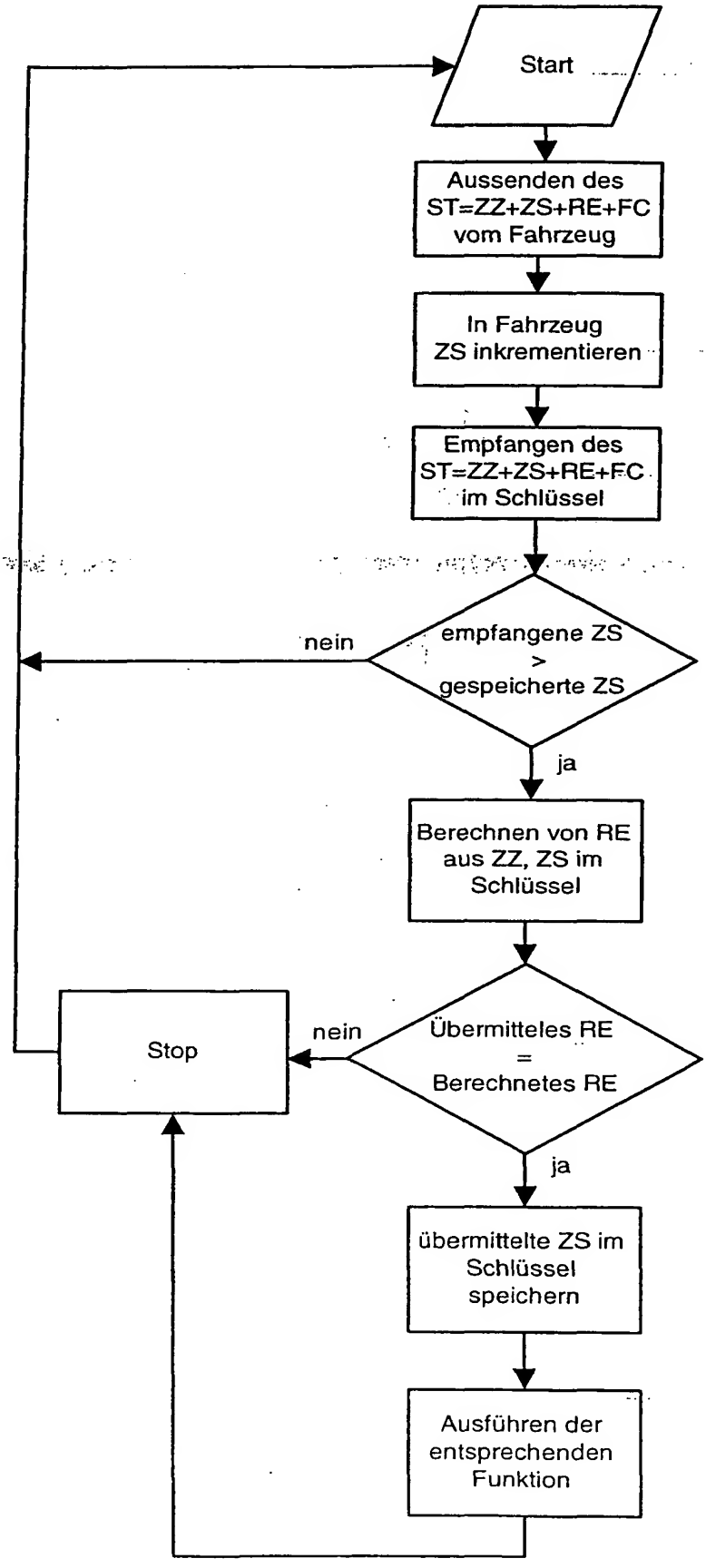
Start
Aussenden des ST=ZZ+ZS+RE+FC vom Fahrzeug
In Fahrzeug ZS inkrementieren
Empfangen des ST=ZZ+ZS+RE+FC im Schlüssel
empfangene ZS > gespeicherte ZS
nein
ja
Berechnen von RE aus ZZ, ZS im Schlüssel
Übermitteles RE = Berechnetes RE
nein
ja
Stop
übermittelte ZS im Schlüssel speichern
Ausführen der entsprechenden Funktion

Fig. 1